

RingCentral Router Configuration

Basic Start Guide for Administrators



Contents

3	Getting Started	24	Tips and Additional Information
4	Quality of Service	25	Tips and Additional Information
4	Test Your Connection Quality & Capacity	25	Media Access Control (MAC)
5	Select Your Router	25	MAC Addresses
6	Select Your Router	25	Find a MAC Address in Windows
7	Configure Your Router	25	Find a MAC Address in UNIX or Linux
8	Configure Your Router	25	Find a MAC Address on the Mac
8	ASUS RT-N66U Dark Knight Configuration	26	Summary - How to Find a MAC Address
9	D-Link HD Media Router 2000	26	How to Change a MAC Address
11	Linksys E1200	26	Summary - Change a MAC Address
17	Linksys E2500	26	Change the Default SSID on Wireless Access Points and Routers
19	Linksys EA4500	27	Find the IP Address of a Network Device
21	How to Set Up a Network Router	27	What's My IP Address?
22	How to Set Up a Network Router	27	How to Find Your IP Address
22	What You Need	27	How to Find Your IP and MAC Addresses On Windows
22	Steps	28	Wi-Fi Network Security Best Practices

Getting Started

Quality of Service

RingCentral provides reliable, high-quality voice service. Your local network, Internet connection, and router all contribute to overall call quality, with high bandwidth being the biggest factor. To help you manage your call quality, RingCentral offers tools to check your Internet connection speed, and instructions to configure the Quality of Service (QoS) settings of your routers.

The Quality of Service (QoS) settings on your router enable it to give priority to voice traffic over lower priority data traffic, such as large downloads. RingCentral has tested and approved a set of QoS-enabled routers for use with RingCentral VoIP services. Recommended routers appear in the next section along with configuration settings to enable QoS on the router device you choose.

Test Your Connection Quality & Capacity

RingCentral provides a [VoIP Quality test](#) that will simulate VoIP calls between your computer and RingCentral, and provide an estimate of the voice quality you should expect when using our service. For the most accurate results, run this test during peak usage times while connected to the network that you plan to use for RingCentral.

A two-minute test is typically sufficient, while longer tests are useful to find intermittent problems or to simultaneously test VoIP performance along with other traffic such as file transfers or remote access.

The RingCentral [Connection Capacity test](#) will help determine the maximum number of simultaneous RingCentral calls that can be supported on your broadband connection. Run this test during normal business hours when the connection is in use by other applications. When the test completes, you will see the recommended number of simultaneous calls your connection can support while maintaining high Quality of Service.



RESULTS SUMMARY

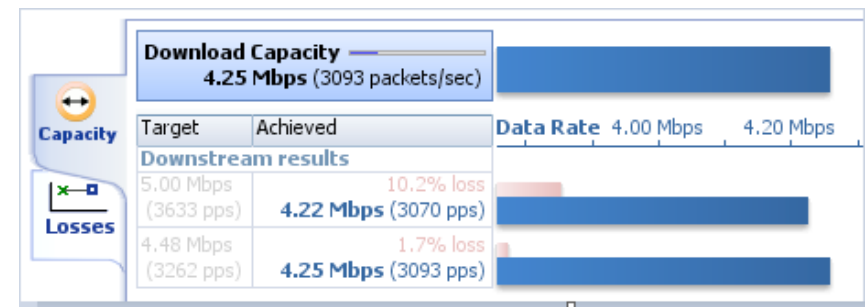
Test audit report



Your connection's [jitter](#) was measured as 1.3ms, which indicates that it can produce a constant flow of data. Voice-over-IP conversations should be of good quality.

Your connection's [packet loss](#) was measured at 0.0%, which indicates that it is accurately transferring data. Voice-over-IP conversations should be of good quality.






Your connection's [MOS score](#) is estimated to be 4.1.



Select Your Router

Select Your Router

RingCentral has taken the “guesswork” out of router selection. Since we know that Quality of Service (QoS) is paramount to your business, we have carefully selected and tested a set of dependable routers suitable for supporting high quality Voice-over-IP conversations. Select your router from the following list. Visit the RingCentral Customer Support Center to learn whether the router you may already own is on the recommended list.

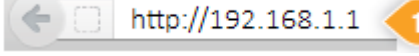
Brand/Model	Wireless	Recommended	# of Users	PDF
ASUS				
RT-N66U Dark Knight	✓	✓	Up to 20	
D-link				
HD Media Router 2000 (827)	✓	✓	Up to 40	
Linksys				
E1200	✓	✓	Up to 12	
E2500	✓	✓	Up to 12	
EA4500	✓	✓	Up to 28	

Configure Your Router

Configure Your Router

ASUS RT-N66U Dark Knight Configuration

Configuring QoS on the ASUS RT-N66U Dark Knight to Prioritize VoIP Traffic

1. Log in to the router. 
Follow the prompts to create a password and a username will be given to you
2. Click **Traffic Manager** on the left hand side.
3. Click on the **QoS** slider to turn QoS on.
4. When the QoS slider turns green, enter your current bandwidth for both the upload and download. (If unsure of your current bandwidth speed, please run a speed test at <http://www.speedtest.net/>.)
5. Click **Save** after entering your bandwidth figures.
6. Be sure to power cycle/reboot the router before proceeding.
7. Your QoS should now be configured.



Brand: ASUS
Model: RT-N66U
Firmware Version: 3.0.0.3.112



D-Link HD Media Router 2000 (DIR 827)

Configuring QoS on the D-Link HD Media Router 2000 to Prioritize VoIP Traffic



Brand: D-Link
Model: HD Media Router 2000
Firmware Version: v 1.04

1. Log in to D-link router. The default IP address is 192.168.0.1.

LOGIN

Log in to the router

User Name : Admin

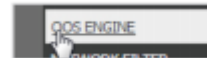
Password :

Log In

2. Click on **ADVANCED**.



3. Click on **QOS ENGINE**.



4. Click on **Enable Traffic Shaping**.

WAN TRAFFIC SHAPING

Enable Traffic Shaping : ☒

5. Enter your broadband provider's uplink speed (1024K in this example). This information is typically listed on your monthly service invoice.

Measured Uplink Speed : 1024 kbps

Manual Uplink Speed : 1024 kbps << Select Transmission Rate

Connection Type : Auto-detect

6. Select all checkboxes in **QOS ENGINE SETUP**.

QOS ENGINE SETUP

Enable QoS Engine : ☒

Automatic Classification : ☒

Dynamic Fragmentation : ☒

7. Add QoS rule for port 5060 – 5090 UDP

Rule name: RC1

Priority 1

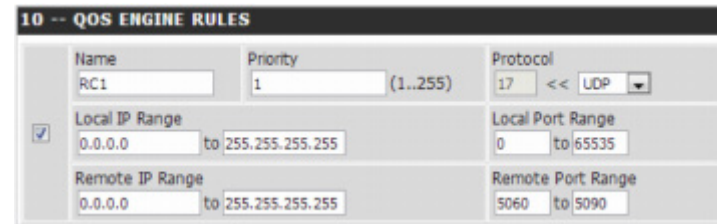
Protocol UDP

Local IP range 0.0.0.0 – 255.255.255.255

Local port range 0 – 65353

Remote IP range 0.0.0.0 – 255.255.255.255

Remote port range 5060 – 5090



The screenshot shows the '10 -- QOS ENGINE RULES' configuration window. It contains a table with one rule, RC1. The rule is enabled (checkbox checked). The configuration fields are: Name: RC1, Priority: 1 (range 1..255), Protocol: 17 (UDP). The Local IP Range is 0.0.0.0 to 255.255.255.255. The Local Port Range is 0 to 65535. The Remote IP Range is 0.0.0.0 to 255.255.255.255. The Remote Port Range is 5060 to 5090.

Name	Priority	Protocol
RC1	1 (1..255)	17 << UDP

☒ Local IP Range: 0.0.0.0 to 255.255.255.255

☒ Local Port Range: 0 to 65535

☒ Remote IP Range: 0.0.0.0 to 255.255.255.255

☒ Remote Port Range: 5060 to 5090

8. Add QoS rule for port 5060 – 5090 UDP

Rule name: RC2

Priority 1

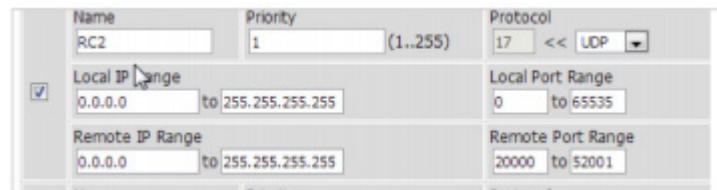
Protocol UDP

Local IP range 0.0.0.0 – 255.255.255.255

Local port range 0 – 65353

Remote IP range 0.0.0.0 – 255.255.255.255

Remote port range 20000 – 52001



The screenshot shows the '10 -- QOS ENGINE RULES' configuration window. It contains a table with one rule, RC2. The rule is enabled (checkbox checked). The configuration fields are: Name: RC2, Priority: 1 (range 1..255), Protocol: 17 (UDP). The Local IP Range is 0.0.0.0 to 255.255.255.255. The Local Port Range is 0 to 65535. The Remote IP Range is 0.0.0.0 to 255.255.255.255. The Remote Port Range is 20000 to 52001.

Name	Priority	Protocol
RC2	1 (1..255)	17 << UDP

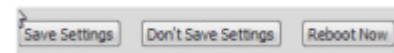
☒ Local IP Range: 0.0.0.0 to 255.255.255.255

☒ Local Port Range: 0 to 65535

☒ Remote IP Range: 0.0.0.0 to 255.255.255.255

☒ Remote Port Range: 20000 to 52001

9. Save Settings and click Reboot Now.



The screenshot shows the bottom of the configuration window with three buttons: 'Save Settings', 'Don't Save Settings', and 'Reboot Now'.

Save Settings Don't Save Settings Reboot Now

Linksys E1200

Configuring QoS on the Linksys E1200 to Prioritize VoIP Traffic (MAC Method)

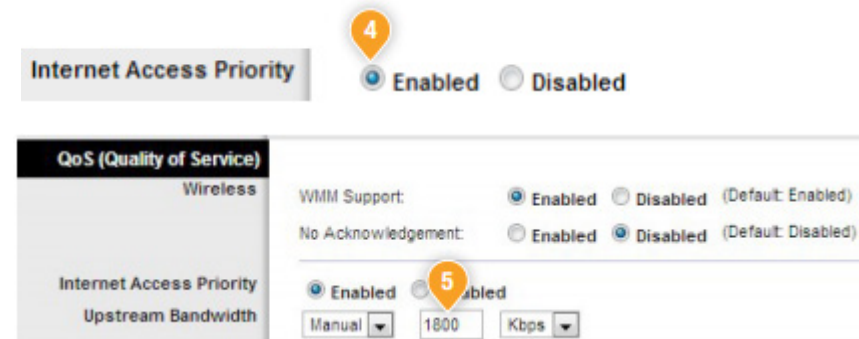


Brand: Linksys
Model: E1200
Firmware Version: 2.0.04 build 1

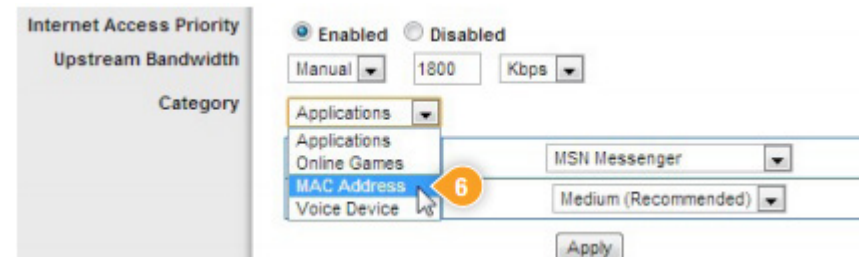
1. Log in to the router. The default IP address is 192.168.1.1. The default username is **admin**. The default password is **admin**.
2. Click on **Applications & Gaming** tab.
3. Click on **QoS**.



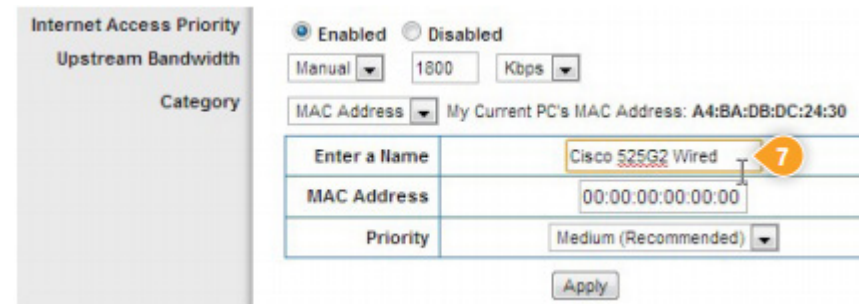
4. Select the radio button **Enabled** next to the field labeled **Internet Access Priority**.
5. In the field labeled **Upstream Bandwidth**, select **Manual** from the drop-down menu and enter your current upload speed. (If unsure of your current upload speed, please run a speed test at <http://www.ringcentral.com/support/capacity.html>)



6. Select **MAC Address** from the drop-down menu labeled **Category**.

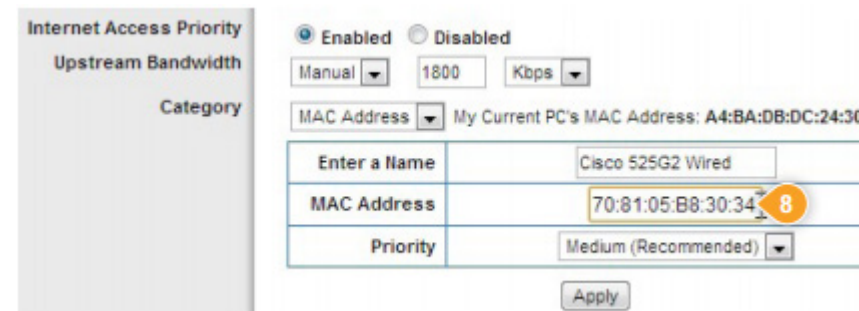


7. You will need the MAC address for each IP device to continue. In the field labeled **Enter a Name**, enter a unique name for the device for which you will prioritize traffic.



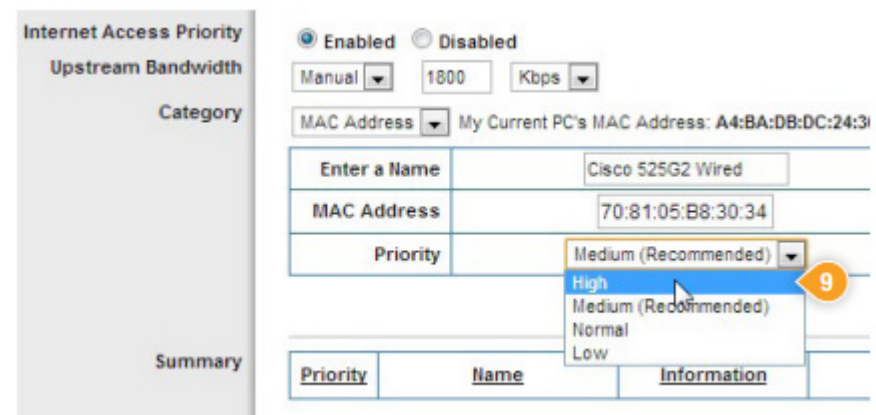
The screenshot shows the 'Internet Access Priority' configuration page. The 'Enabled' radio button is selected. The 'Upstream Bandwidth' is set to 'Manual' with a value of '1800' and units of 'Kbps'. The 'MAC Address' dropdown is set to 'My Current PC's MAC Address: A4:BA:DB:DC:24:30'. The 'Enter a Name' field contains 'Cisco 525G2 Wired' and is highlighted with an orange box and a red circle with the number 7. The 'MAC Address' field contains '00:00:00:00:00:00'. The 'Priority' dropdown is set to 'Medium (Recommended)'. An 'Apply' button is at the bottom.

8. In the field labeled **MAC Address** enter the MAC address for the device.



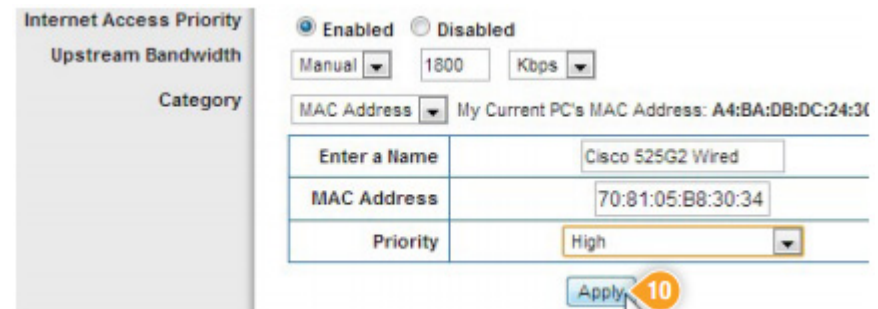
The screenshot shows the 'Internet Access Priority' configuration page. The 'Enabled' radio button is selected. The 'Upstream Bandwidth' is set to 'Manual' with a value of '1800' and units of 'Kbps'. The 'MAC Address' dropdown is set to 'My Current PC's MAC Address: A4:BA:DB:DC:24:30'. The 'Enter a Name' field contains 'Cisco 525G2 Wired'. The 'MAC Address' field contains '70:81:05:B8:30:34' and is highlighted with an orange box and a red circle with the number 8. The 'Priority' dropdown is set to 'Medium (Recommended)'. An 'Apply' button is at the bottom.

9. In the field labeled **Priority**, select **High** from the drop-down menu



The screenshot shows the 'Internet Access Priority' configuration page. The 'Enabled' radio button is selected. The 'Upstream Bandwidth' is set to 'Manual' with a value of '1800' and units of 'Kbps'. The 'MAC Address' dropdown is set to 'My Current PC's MAC Address: A4:BA:DB:DC:24:30'. The 'Enter a Name' field contains 'Cisco 525G2 Wired'. The 'MAC Address' field contains '70:81:05:B8:30:34'. The 'Priority' dropdown is open, showing options: 'Medium (Recommended)', 'High', 'Medium (Recommended)', 'Normal', and 'Low'. The 'High' option is highlighted with an orange box and a red circle with the number 9. Below the dropdown is a table with columns 'Priority', 'Name', and 'Information'.

10. Click **Apply** to save changes.



Internet Access Priority

Upstream Bandwidth

Category

☒ Enabled ☐ Disabled

Manual Kbps

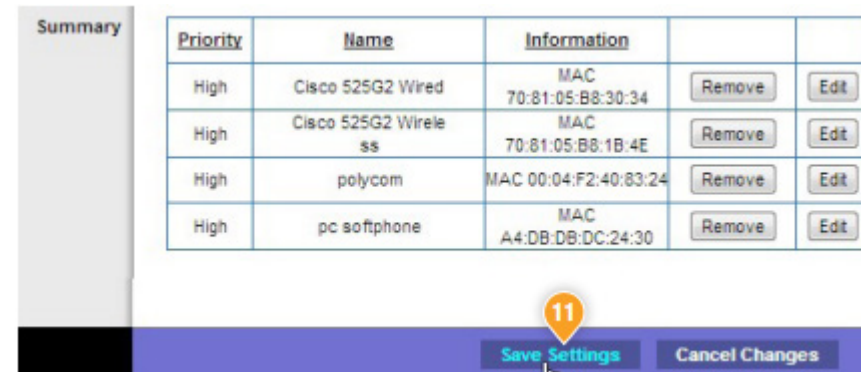
MAC Address

Enter a Name	<input type="text" value="Cisco 525G2 Wired"/>
MAC Address	<input type="text" value="70:81:05:B8:30:34"/>
Priority	<input type="text" value="High"/>

Apply **10**

11. Repeat steps 6-10 until you have entered all of the IP phones. When all have been entered and you see them in the **Summary** section, click on **Save Settings**.

12. Power cycle/reboot the router before proceeding.



Summary

Priority	Name	Information		
High	Cisco 525G2 Wired	MAC 70:81:05:B8:30:34	Remove	Edit
High	Cisco 525G2 Wireless	MAC 70:81:05:B8:1B:4E	Remove	Edit
High	polycom	MAC 00:04:F2:40:83:24	Remove	Edit
High	pc softphone	MAC A4:DB:DB:DC:24:30	Remove	Edit

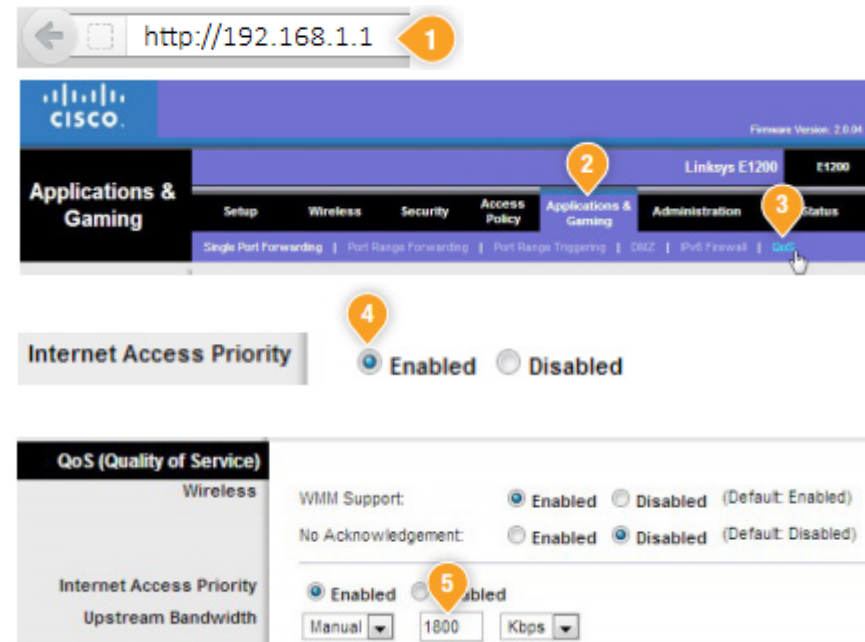
11

Save Settings Cancel Changes

Linksys E1200

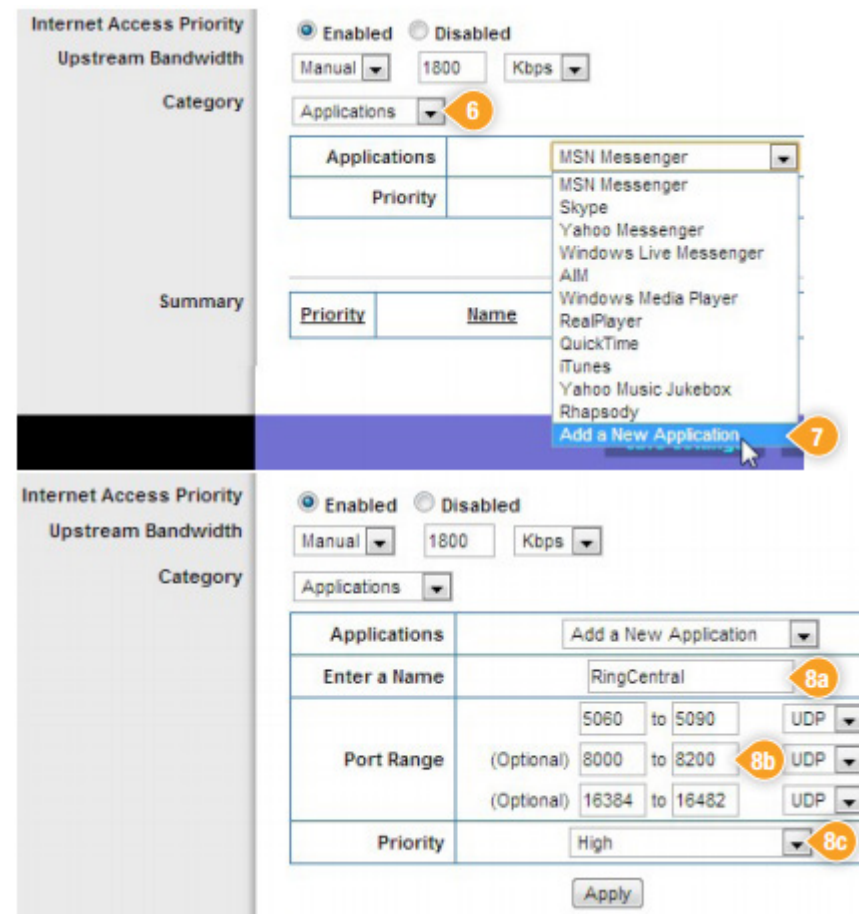
Configuring QoS on the Linksys E1200 to Prioritize VoIP Traffic (Port Method)

1. Log in to the router. The default IP address is 192.168.1.1. The default username is **admin**. The default password is **admin**.
2. Click on **Applications & Gaming** tab.
3. Click on **QoS**.
4. Select the radio button **Enabled** next to the field labeled Internet Access Priority.
5. In the field labeled **Upstream Bandwidth**, select **Manual** from the drop-down menu and enter your current upload speed. (If unsure of your current upload speed, please run a speed test at <http://www.ringcentral.com/support/capacity.html>.)



6. In the **Category** section, select **Applications** from the drop-down menu.
7. In the field labeled **Applications**, select **Add a New Application** from the drop-down menu.

8. Enter a unique name in the **Enter a Name** field. Enter the following port ranges and select **UDP** from the drop-down menu to the right of each port range field and set the priority to **High** on the drop-down menu: **5060-5090**, **8000-8200**, **16384-16482**.



Internet Access Priority

Upstream Bandwidth

Category

Summary

Enabled ☒ Disabled ☐

Manual 1800 Kbps

Applications 6

Applications

Priority

MSN Messenger

MSN Messenger

Skype

Yahoo Messenger

Windows Live Messenger

AIM

Windows Media Player

RealPlayer

QuickTime

iTunes

Yahoo Music Jukebox

Rhapsody

Add a New Application 7

Internet Access Priority

Upstream Bandwidth

Category

Enabled ☒ Disabled ☐

Manual 1800 Kbps

Applications

Applications

Enter a Name

Port Range

Priority

5060 to 5090 UDP 8a

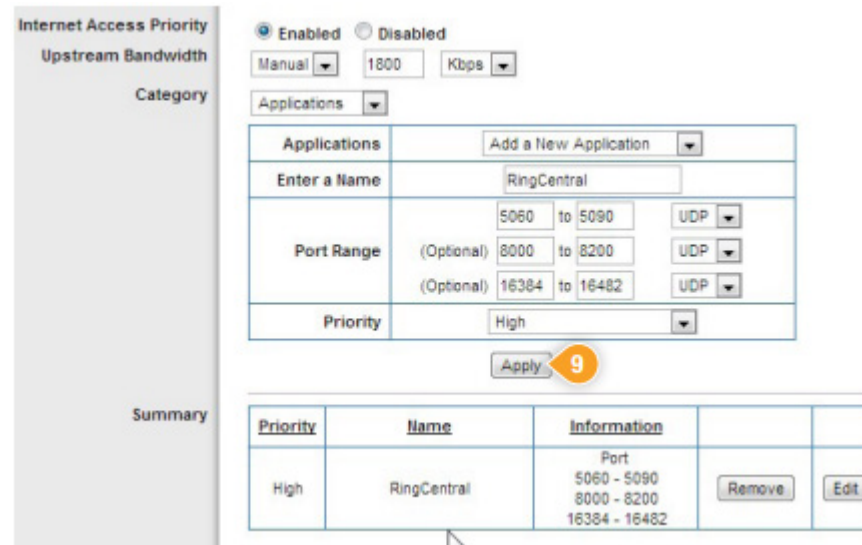
(Optional) 8000 to 8200 8b UDP

(Optional) 16384 to 16482 8b UDP

High 8c

Apply

9. Click **Apply**. You will see your changes in the **Summary** section.



Internet Access Priority

Upstream Bandwidth

Category

Enabled ☒ Disabled ☐

Manual Kbps

Applications

Applications	Enter a Name	Port Range	Protocol
	RingCentral	5060 to 5090	UDP
		(Optional) 8000 to 8200	UDP
		(Optional) 16384 to 16482	UDP
		Priority	High

Apply **9**

Priority	Name	Information		
High	RingCentral	Port 5060 - 5090 8000 - 8200 16384 - 16482	Remove	Edit

10. Click on **Save Settings**.

11. Power cycle/reboot the router before proceeding.



Summary

Priority	Name	Information		
High	RingCentral	Port 5060 - 5090 8000 - 8200 16384 - 16482	Remove	Edit

10

Save Settings Cancel Changes

Linksys E2500

Configuring QoS on the Linksys E2500 to Prioritize VoIP Traffic

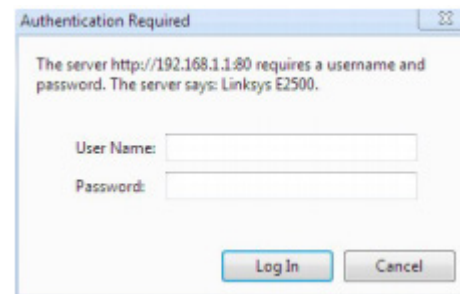


Brand: Linksys

Model: E2500

Firmware Version: 1.0.07

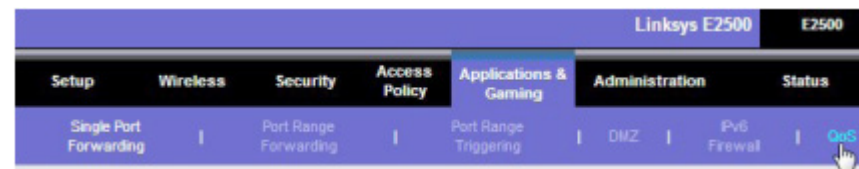
1. Log in to Linksys router.



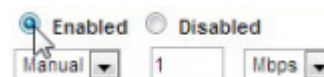
2. Select **Applications & Gaming**.



3. Click on **QoS**.



4. Select **Enabled** to enable QoS service. Enter your broadband provider's uplink speed. This information is typically listed on your monthly service invoice. It's 1Mbps in our example.



5. Select **MAC** address. Set **Priority** to **High**.

MAC Address ▼ My Current PC's MAC Address: A4:BA:DB:DC:24:30

Enter a Name	<input type="text"/>
MAC Address	<input type="text" value="00:00:00:00:00:00"/>
Priority	Medium (Recommended) ▼

Apply

6. Enter the **Name** of your device and **MAC Address** of each phone. The MAC Address can be found on the back of your device or in the device menu.

Enter a Name	<input type="text" value="Telcolab1"/>
MAC Address	<input type="text" value="00:01:02:62:4A:D1"/>
Priority	High (Recommended) ▼

Apply

7. Save Settings.

Priority	Name	Information		
High	Telcolab1	MAC 00:01:02:62:4A:D1	Remove	Edit

Save Settings

Cancel Changes

8. Select **Continue** to finish and return to the configuration menu.

Your settings have been successfully saved.

Continue

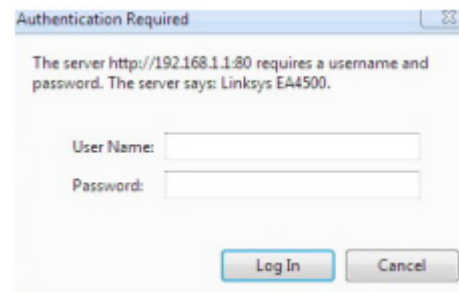
Linksys EA4500

Configuring QoS on the Linksys EA4500 to Prioritize VoIP Traffic

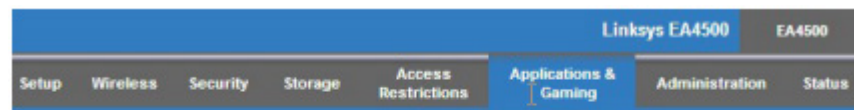


Brand: Linksys
Model: EA4500
Firmware Version: 4.21.5

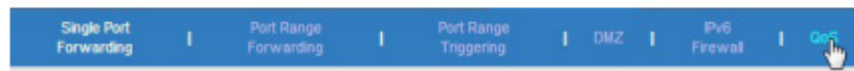
1. Log in to Linksys router.



2. Select **Applications & Gaming**.



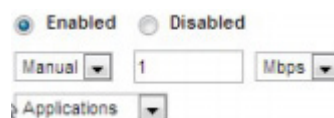
3. Click on **QoS**.



4. Select **Enabled** to enable **QoS** service. Enter your broadband provider's uplink speed. This information is typically listed on your monthly service invoice. It's 1Mbps in our example.



5. Select **Applications** from the category menu.



6. Enter an application name and select **Priority High**.

Enter the following port range:

Port Range: 20000 – 65535 Protocol: UDP

Port Range: 5060 – 5090 Protocol: UDP

Click on Apply to save settings.

Applications ▼

Applications	Add a New Application ▼		
Enter a Name	RingCentral		
Port Range	20000 to 65535	UDP ▼	
	(Optional) 5060 to 5090	UDP ▼	
	(Optional) to	Both ▼	
Priority	High ▼		

Apply

7. Click on **Save Settings** to finish your setup.

Priority	Name	Information		
High	RingCentral	Port 20000 - 65535 5060 - 5090	Remove	Edit

Save Settings Cancel Changes

8. Select **Continue** to finish and return to the router configuration screen.

Your settings have been successfully saved.

Continue

How to Set Up a Network Router

How to Set Up a Network Router

This section explains how to set up a router for office computer networks. The exact names of configuration settings on a network router vary depending on the model and whether it is wired or wireless. However, this general procedure will guide you through the process for the common kinds of network equipment

What You Need

- A network router (wireless or wired)
- Network adapters installed on all devices to be connected to the router
- A working Internet modem (optional)
- A Web browser installed at least one computer in the network

Steps

1. Choose a convenient location to begin installing your router such as an open floor space or table. This does not need to be the permanent location of the device. Particularly for wireless routers, you may find it necessary to re-position the unit after installing it as the cables / signals may not reach all areas needed. At the beginning, it's better to choose a location where it's easiest to work with the router and worry about final placement later.
2. Plug in the router's electrical power source; then turn on the router by pushing the power button.
3. (Optional) Connect your Internet modem to the router. Most network modems connect via an Ethernet cable but USB connections are becoming increasingly common. The cable plugs into the router jack

named **WAN** or **uplink** or **Internet**. After connecting the cable, be sure to power cycle (turn off and turn back on) the modem to ensure the router recognizes it.

4. Connect one computer to the router, by cable or wirelessly. The routers recommended by RingCentral are capable of reliable connection by either method.
5. Open the router's administration tool. From the computer connected to the router, first open your Web browser. Then enter the router's address for network administration in the Web address field and hit return to reach the router's home page.
Many routers are reached by either the Web address <http://192.168.1.1> or <http://192.168.0.1>. Consult your router's documentation to determine the exact address for your model. Note that you do not need a working Internet connection for this step.
6. Log in to the router. The router's home page will ask you for a username and password. Both are provided in the router's documentation. You should change the router's password for security reasons, but do this after the installation is complete to avoid unnecessary complications during the basic setup.
7. If you want your router to connect to the Internet, you must enter Internet connection information into that section of the router's configuration (exact location varies). If using DSL Internet, you may need to enter the PPPoE username and password. Likewise, if you have been issued a static IP address by your provider (you would need to have requested it), the static IP fields (including network mask and gateway) given to you by the provider must also be set in the router.
8. If you were using a primary computer or an older network router to connect to the Internet, your provider may require you to update the MAC address of the router with the MAC address of the device you were using previously. Read [How to Change a MAC Address](#) for a detailed description of this process.

9. If this is a wireless router, change the network name (often called SSID). While the router comes to you with a network name set at the factory, you will never want to use this name on your network. Read [Change the Default SSID on Wireless Access Points and Routers](#) for detailed instructions.
10. Verify the network connection is working between your one computer and the router. To do this, you must confirm that the computer has received IP address information from the router. See [Find the IP Address of a Network Device](#) for a description of this process.
11. (If applicable) Verify your one computer can connect to the Internet properly. Open your Web browser and visit a few Internet sites such as <http://compnetworking.about.com/>.
12. Connect additional computers to the router as needed. If connecting wirelessly, ensure the network name (SSID) of each computer matches that of the router.
13. Finally, configure additional network security features as desired to guard your systems against Internet attackers. These [Wi-Fi Network Security Best Practices](#) offer a good checklist to follow.

Tips and Additional Information

Tips and Additional Information

When connecting devices with network cables, be sure each end of the cable connects tightly. Loose cables are one of the most common sources of network setup problems.

Media Access Control (MAC)

MAC technology provides unique identification and access control for computers on an Internet Protocol (IP) network. In wireless networking, MAC is the radio control protocol on the wireless network adapter. Media Access Control works at the lower sub-layer of the data link layer (Layer 2) of the OSI model.

MAC Addresses

Media Access Control assigns a unique number to each IP network adapter called the MAC address. A MAC address is 48 bits long. The MAC address is commonly written as a sequence of 12 hexadecimal digits as follows:

48-3F-0A-91-00-BC

MAC addresses are uniquely set by the network adapter manufacturer and are sometimes called physical addresses. The first six hexadecimal digits of the address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number. MAC addresses map to logical IP addresses through the Address Resolution Protocol (ARP).

Some Internet service providers track the MAC address of a router for security purposes. Many routers support a process called cloning that allows the MAC address to be simulated so that it matches one the service provider is expecting. This allows households to change their router (and their real MAC address) without having to notify the provider.

The method used to find a MAC address depends on the type of network device involved. All popular network operating systems contain utility

programs that allow you to find (and sometimes change) MAC address settings.

Find a MAC Address in Windows

Use the ipconfig utility (with the /all option) to display the computer's MAC address in modern versions of Windows. Very old versions like Windows 95 and Windows 98 used the winipcfg utility instead.

Both 'winipcfg' and 'ipconfig' may display multiple MAC addresses for one computer. One MAC address exists for each installed network card. Additionally, Windows maintains one or more MAC addresses that are not associated with hardware cards.

For example, Windows dial-up networking uses virtual MAC addresses to manage the phone connection as if it were a network card. Some Windows VPN clients likewise have their own MAC address. The MAC addresses of these virtual network adapters are the same length and format as true hardware addresses.

Find a MAC Address in UNIX or Linux

The specific command used in UNIX to find a MAC address varies depending on the version of the operating system. In Linux and in some forms of UNIX, the command ifconfig -a returns MAC addresses.

You can also find MAC addresses in UNIX and Linux in the boot message sequence. These operating systems display the computer's MAC address on-screen as the system reboots. Additionally, boot-up messages are retained in a log file (usually "/var/log/messages" or "/var/adm/messages").

Find a MAC Address on the Mac

You can find MAC addresses on Apple Mac computers in the TCP/IP Control Panel. If the system is running Open Transport, the MAC address appears under the "Info" or "User Mode/Advanced" screens. If the system is running MacTCP, the MAC address appears under the "Ethernet" icon.

Summary - How to Find a MAC Address

The list below summarizes options to find a computer's MAC address:

- Windows: ipconfig /all, or winipcfg
- Linux and some Unix: ifconfig -a
- Mac with Open Transport: TCP/IP Control Panel - Info or User Mode/Advanced
- Mac with MacTCP: TCP/IP Control Panel - Ethernet icon
- MAC addresses were designed to be fixed numbers that cannot be changed. However, there are several valid reasons to want to change your MAC address

How to Change a MAC Address

Most Internet subscriptions allow the customer only a single IP address. The Internet Service Provider (ISP) may assign one static (fixed) IP address to each customer. However, this approach is an inefficient use of IP addresses that are currently in short supply. The ISP more commonly issues each customer dynamic IP address that may change each time the customer connects to the Internet.

ISPs ensure each customer receives only one dynamic address using several methods. Dial-up and many DSL services typically require the customer to log in with a username and password. Cable modem services, on the other hand, do this by registering and tracking the MAC address of the device that connects to the ISP.

The device whose MAC address is monitored by an ISP can be the cable modem, a broadband router, or the PC that hosts the Internet connection. The customer is free to build a network behind this equipment, but the ISP expects the MAC address to match the registered value at all times.

Whenever a customer replaces that device, however, or changes the network adapter inside it, the MAC address of this new equipment will

no longer match the one registered at the ISP. The ISP will often disable the customer's Internet connection for security (and billing) reasons.

Summary - Change a MAC Address

The MAC address is an important element of computer networking. MAC addresses uniquely identify a computer on the LAN. MAC is an essential component required for network protocols like TCP/IP to function.

Computer operating systems and broadband routers support viewing and sometimes changing MAC addresses. Some ISPs track their customers by MAC address. Changing a MAC address can be necessary in some cases to keep an Internet connection working. Some broadband modems also monitor the MAC address of their host computer.

Although MAC addresses do not reveal any geographic location information like IP addresses do, changing MAC addresses may improve your Internet privacy in some situations.

Change the Default SSID on Wireless Access Points and Routers

Wi-Fi access points and routers establish a wireless network using a name called an SSID (Service Set Identifier). Routers are configured with a default SSID pre-defined and set by the manufacturer at the factory.

Typical default SSIDs are simple names like

- "wireless"
- "netgear"
- "linksys"
- "default"

The SSID can be accessed from within the router's Web-based or Windows-based configuration utilities. It can be changed at any time,

but wireless clients must then recognize the new SSID in order to reconnect to that router and wireless network.

To improve the security of your wireless network, consider changing the router's SSID to a different name than the default. Here are some recommended do's and don'ts, based on recommended network security practices:

- Don't embed your name, address, birth date, or other personal information as part of the SSID
- Likewise, don't use any of your Windows or Internet web site passwords
- Don't tempt would-be intruders by using tantalizing network names like "SEXY-BOX" or "TOP-SECRET"
- Do pick an SSID that contains both letters and numbers
- Do choose a name as long or nearly as long as the maximum length allowed
- Do consider changing your SSID periodically (at least once every few months)
- Do disable SSID broadcast on your network; make users manually find it.

Find the IP Address of a Network Device

Every computer or other device connected to the Internet or other IP network is given at least one IP address. Various methods exist to find the IP addresses of your computer, your router, or even someone else's web site or other network equipment in some cases

What's My IP Address?

A network may contain multiple computers or other devices each having their own IP address (or addresses). Answering the question "What's My IP Address?" depends on exactly which one(s) you seek.

How to Find Your IP Address

Follow these guidelines to find your IP network address (or addresses) in different situations. It's not difficult once you know where to look.

How to Find Your IP and MAC Addresses On Windows

Follow these steps to quickly find the Internet Protocol (IP) and Media Access Control (MAC) address of a computer running Microsoft Windows XP, Windows Vista, or Windows 7.

1. Click go to Start > All Programs > Accessories > Command Prompt.
2. If not at the C: root, type C: at the flashing prompt.
3. At C: type "ipconfig /all" (minus the quotes). Details are shown for each of the computer's network adapters. Computers installed with VPN software or emulation software will possess one or more virtual adapters.
4. The "IP Address" field states the current IP address for that network adapter.
5. The "Physical Address" field states the MAC address for that adapter.

Tips:

1. Take care to read the IP address from the correct adapter. Virtual adapters generally show a private address rather than an actual Internet address.
2. Virtual adapters possess software-emulated MAC addresses and not the actual physical address of the network interface card.

What You Need

- Microsoft Windows XP or newer version of the operating system

Wi-Fi Network Security Best Practices

Many folks setting up wireless networks rush through the job to get their Internet connectivity working as quickly as possible. That's totally understandable. It's also quite risky as numerous security problems can result. Today's Wi-Fi networking products don't always help the situation as configuring their security features can be time-consuming and non-intuitive. The recommendations below summarize the steps you should take to improve the security of your wireless network.

1. Change Default Administrator Passwords (and Usernames)

At the core of most Wi-Fi networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

2. Turn on (Compatible) WPA / WEP Encryption

All Wi-Fi equipment supports some form of encryption. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting.

3. Change the Default SSID

All Wi-Fi equipment supports some form of encryption. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form

of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting.

4. Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the physical address or MAC address. Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their equipment, which restricts the network to only allow connections from those devices. Do this, but also know that the feature is not as powerful as it may seem. Hackers and their software programs can fake MAC addresses easily.

5. Disable SSID Broadcast

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. Most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator.

6. Do Not Auto-Connect to Open Wi-Fi Networks

Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should not be enabled except in temporary situations.

7. Assign Static IP Addresses to Devices

Most network devices permit using dynamic IP addresses. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range instead, and then configure each connected device to match. Use a private IP address range

(like 10.0.0.x) to prevent computers from being directly reached from the Internet.

8. Enable Firewalls On Each Computer and the Router

Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running additional firewall software on each computer connected to the router.

9. Position the Router or Access Point Safely

Wi-Fi signals often reach to the exterior of a building. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach through neighboring businesses and into streets, for example. When installing a wireless network, the position of the access point or router determines its reach. Try to position these devices near the center of the building rather than near windows to minimize leakage.

10. Turn Off the Network During Extended Periods of Non-Use

While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods offline.

If you own a wireless router but are only using it wired (Ethernet) connections, you can also sometimes turn off Wi-Fi on a broadband router without powering down the entire network.